# Commander, Navy Installations

# Common Access Card
# Personal Identification Number Reset
# (CPR)
# Business Policy Statement

**November 2004**
**Version 1.1**

# Table of Contents

# 1. INTRODUCTION

## 1.1. Overview

This document prescribes the Navy's business policy for the fielding, management, use and maintenance of the Common Access Card (CAC) Personal Identification Number (PIN) Reset system (hereafter referred to as CPR).

## 1.2. Background

The Real-time Automated Personnel Identification System (RAPIDS) was established in 1981 to provide a secure, automated method of producing identification (ID) cards; and upgraded in 2000 to support the issuance and update of the Department of Defense (DoD) CAC.

The CAC is an ID card with an integrated circuit chip (ICC) for processing and storing information. The CAC initial issuance was achieved through the Defense Enrollment Eligibility Reporting System (DEERS)/RAPIDS workstations under the control of Verifying Officials (VOs).

The CAC has a Personal Identification Number (PIN) known only to the cardholder. The PIN is a 6-to-8 digit number the cardholder enters at issuance. To use any certificates or applets resident on the card, the cardholder must supply the PIN.

a. Upon CAC insertion into a card reader, the workstation middleware attempts to access a card applet.

b. The cardholder is prompted to enter a PIN.

c. The entered PIN is validated against the PIN stored on the card.
    - If the PIN is *correct*, the card is available for use.
    - If the PIN is *incorrect*, the cardholder has three attempts to provide the correct PIN. After the third unsuccessful attempt, the card's PIN management applet *locks* the CAC. Access to certificates and data.on the CAC is restricted until the PIN has been reset.

Due to inherent programmatic delays between CAC issuance and fielding card readers and middleware components to the desktop environment, users often tended to forget their PINs, resulting in numerous cases of *locked* CACs. This resulted in several problems:

- To reactivate the CACs, users needed to travel to a RAPIDS issuance facility, wait for DEERS/RAPIDS workstation availability, and then have their PINs reset.
- This approach resulted in both a loss of user productivity and diversion of RAPIDS personnel and resources from their primary mission, card issuance.
- The RAPIDS issuance facilities are not staffed to provide 24-hour support, making timely PIN reset more difficult.

### 1.3. Purpose

The CPR system provides a portable, flexible, single-purpose system capable of providing timely PIN reset capability to the field in a myriad of operating environments. This system securely solves the PIN reset problems using Commercial off the Shelf (COTS) hardware over a non NMCI network and requires minimal user training.

### 1.4. Document Organization

This business policy statement provides compliance requirements for CPR system users, namely supporting infrastructure management and CPR workstation users. It is not intended as a user's manual for day-to-day CPR operation. Detailed procedures regarding policy compliance are available through the CAC PIN Reset Standard Operating Procedures and Users' Guide.

### 1.5. Related Documents

This policy incorporates requirements specified in the following documents:

- X.509 Certificate Policy for the United States Department of Defense, Version 7.0, December 2002
- Department of Defense (DoD) Real-time Automated Personnel Identification System (RAPIDS) Workstation and Verifying Official (VO) Certification Practice Statement (CPS), Version 2.0, September 2001

### 1.6. Contact Details

#### 1.6.1. Specification Administration Organization

CNI CAC Program Management Office (CAC PMO) is responsible for maintaining this Business Process Policy Statement.

#### 1.6.2. Contact Information

For questions regarding this policy statement contact the CNI, CAC Program Management Office, CPR project officer, (850) 452-7715.

## 2. Roles and Responsibilities

### 2.1. Defense Manpower Data Center (DMDC)

The DMDC (as the DEERS/RAPIDS administrator) is chartered with maintaining and overseeing efficient operation of the CPR infrastructure.

DMDC responsibilities are specified in the CPR Memorandum of Agreement (MOA) which is available on the CAC PMO website https://pmo.cac.navy.mil.

### 2.2. Commander, Navy Installations (CNI)

CNI, CAC Program Management Office is the functional proponent of the U.S. Navy for the CPR system. The CAC Program Management Office serves as the single organization for centralized operational control of CAC programs and associated electronic transaction systems. Specifically, it is responsible for managing the CPR program Navy-wide, funding and administering associated pilot projects, serving as a clearinghouse for CPR best practices, assisting in the development of applicable implementation plans and coordinating with DMDC as required.

The CNI CAC PMO retains overall responsibility for management of the CPR system for the U.S. Navy and the development, coordination and promulgation of guidance necessary to implement and sustain CPR system operation as well as overall programmatic planning, programming, budgeting and procurement process oversight.

### 2.3. CAC Program Management Office, CPR Project Officer

The CPR Project Officer is the focal point for day-to-day CPR management and administration for CPR. This office works closely with DMDC to ensure the smooth, efficient operation of all CPR-related architectures and processes.

The CPR Project Officer duties include:

- Coordinates initial access to DEERS/RAPIDS
- Approves requests for new or additional site CPR capability
- Coordinates with site TASMs to arrange the acquisition, building and shipment/relocation of CPR workstations or replacement components
- Coordinates with the DEERS Security Team (DST) to register and/or remove site IDs and TASMs
- Provides help desk support to field sites to facilitate CPR component maintenance, servicing and replacement
- Administers the CPR Management Service (CPR-MS), including entering and updating Site Identification numbers, Trusted Agent Security Managers (TASMs) and DEERS data
- Manages the CPR site Locator (through CPR-MS)
- Develops CPR training materials for TASMs and CPR Trusted Agents (CTAs)
- Develops service-specific policy and associated user & administrator manuals

- Meets POC position requirements specified in Section 7.3.1.1
- Approves registration and revocation requests for TASMs
- Coordinates requests for new or additional site CPR capability
- Oversees site ID survey completion within their area of responsibility
- Coordinates replacement part issue and shipment arrangements for CPR workstations
- Provides training and field support services to sites (TASMs) as required

### 2.4. Trusted Agent Security Manager (TASM)

TASMs are responsible for CPR user management, workstation maintenance and administration, and equipment storage and accountability at their specific site. The local Commander (or designated representative) appoints each site TASM.

Each site has two TASMs—a primary and an alternate. TASMs are responsible for:

- Meeting TASM position requirements specified in Section 7.3.1.2
- Adhering to CPR workstation security and equipment access requirements
- Overseeing site survey completion within their area of responsibility
- Managing all TASM and CTAs at their site
- Coordinating replacement parts and shipment arrangements for CPR workstations
- Providing training and field support services to alternate TASMs and CTAs as required
- Providing visibility for the CPR program at their site. The TASM may accomplish this via the site Plan of the Day/Week, newsletter, website, or any other effective means. Information should include the CPR location, hours of operation, telephone numbers, and other pertinent data.
- Coordinating CPR matters to include requests for new or additional CPR site
- Securing and retaining property accountability of all site CPR equipment
- Notifying the CPR project officer or help desk of any CPR capability loss or suspected or known CPR system compromise
- Transmitting audit files created on the CPR workstation to the CPR project officer for sampling and measurement
- Ensuring positive identification of all site CTAs and Subscribers requesting CPR
- Protecting PIN information, including their own, CTAs, and subscribers during the reset process
- Referring subscribers to their CAC issuance facility when unable to perform authentication or conduct PIN reset

### 2.5. CPR Trusted Agent (CTA)

The CTA's primary role in the field is to provide CPR. The TASM (or designated representative) nominates the CTA. CTAs are responsible for:

- Meeting CTA position requirements as specified in Section 7.3.1
- Adhering to CPR workstation security and equipment access requirements
- Performing CAC PIN Reset
- Ensuring positive identification of all subscribers requesting CAC PIN Reset
- Securing and retaining property accountability of all CPR equipment under their control
- Notifying the TASM or CPR Project Officer of any site capability loss, suspected CPR system compromise and/or any malfunctions or anomalies with CPR equipment (CTAs should contact the CAC PMO when the local TASM is unavailable)
- Protecting PIN information, including their own, and subscribers during CPR
- Directing subscribers to their CAC issuance facility when either authentication can not be positively confirmed or the PIN cannot be reset

# 3. Training

## 3.1. TASMs

### 3.1.1. Primary TASM Training

Primary TASMs are considered the priority CPR site user. Primary TASM training can be accomplished by:

- **Regional training** – Conducted at a location near the TASM's site using material developed by CAC PMO in concert with functional CPR workstations, which are distributed to the TASMs after course completion.
- **Electronic media training** – Provided to the TASM directly by CAC PMO, this training may either take the form of computer-based training or non-multimedia format (such as Microsoft PowerPoint® or Microsoft Word® files).

### 3.1.2. Alternate TASM Training

An alternate TASM must be assigned to assist the primary TASM after establishing CPR site capability. Once entered into the CPR system as TASM alternates, they hold the same rights and authorities as the primary TASMs.

The primary TASM provides training to the alternate TASM via on-the-job instruction. No formalized training exists outside of the training materials and support provided by CAC PMO.

## 3.2. CTAs

A TASM provides CTAs with on-the-job training. No formalized training exists outside of the training materials and support provided by CAC PMO.

## 3.3. Training Material Availability

The CAC PMO distributes approved CPR training materials. This is provided in person, via CD-ROM (mailed via the postal system or recognized delivery service) or email.

## 3.4. Acknowledgement of Responsibilities

All TASMs and CTAs receiving CPR user training must complete and sign an Acknowledgement of Responsibilities Form. By completing this form (see Appendix E), TASMs and CTAs acknowledge that they have received CPR training and that they understand their obligations as specified in this policy statement. The form must be completed in the presence of a person who verifies the user's identity and also signs the form.

The original copy of the TASM Acknowledgement Form is forwarded to the CPR Project Officer (via mail, fax, in person, or by digitally signed email). TASMs should retain a local copy.

Acknowledgement forms completed for CTAs may be signed by the TASM conducting the training. TASMs will maintain the original copies of all Acknowledgement forms for CTAs within their site and

forward a copy to the CPR Project Officer (via mail, fax, in person, or by digitally signed email). CTAs may retain a copy for their own records.

Consistent with the requirements specified in the RAPIDS *Verifying Official Certificate Practice Statement*, acknowledgement forms must be retained for a period of 11 years.

For:

- **TASMs** – The CAC PMO maintains these forms (and may also archive them)
- **CTAs** – The site TASM maintains these forms until the CTA no longer performs CPR-related site functions. At that time, the original CTA acknowledgement form is forwarded to the CPR Project Officer for archival.

# 4. General Provisions

## 4.1. Obligations

### 4.1.1. DMDC

The Memorandum of Agreement (MOA) covers obligations between the U.S. Navy and the Defense Manpower Data Center (DMDC). The most current MOA is available on the CAC PMO website (https://www.pmo.cac.navy.mil).

### 4.1.2. CPR Users

CPR users must abide by all obligations defined in this Policy Statement, including personnel controls, technical security controls, and CAC holder authentication rules.

## 4.2. Interpretation and Enforcement

### 4.2.1. Severance of Provisions, Survival, Merger, and Notice

Should any section of this CPR Business Process Policy Statement be determined to be incorrect or invalid, all parties including the CAC PMO, TASMs, CTAs, and CAC holders will nevertheless abide by the practices described herein, until provided new policy guidance.

Invalid information in a section or sections of this document does not invalidate other sections. Thus all other sections of this document should be considered otherwise valid.

### 4.2.2. Dispute Resolution Procedures

The CNI CAC PMO mediates any policy statement disputes regarding interpretation or applicability.

## 4.3. Publication and Repository

### 4.3.1. Publication of POC, TASM, and CTA Information

For the CPR user (TASM and CTA personnel) personal information published in a public location is limited to name, telephone number, email address, and duty location. Under no circumstances is information covered under the Privacy Act of 1974 published in a public directory. This includes information used to populate the CPR-MS for the intent of providing a CPR site locator for the DoN community. Although such information may exist in the CPR-MS database, security safeguards isolate this data from public access.

### 4.3.2. Frequency of Publication

No stipulation.

### 4.3.3. Access Controls

During CPR:

- The Windows 2000 user management security capability and DEERS authentication process controls workstation activity and CPR user access.
- A biometric verification executes for both the CPR user and CAC holder, and involves two approaches:
    - A live fingerprint is compared against DEERS database fingerprint information for both the CPR user and CAC holder. If either verification fails, CPR is not a viable option.
    - A photographic comparison is conducted for the CAC holder.

### 4.3.4. Repositories

The DEERS records all CPR user registrations and PIN reset attempts, and later transmits this information to the CPR Project Officer for CPR-MS inclusion. Local audit files, also created and saved on the CPR workstation, store more detailed information on CPR users and transactions than that stored in the DEERS. These files are sent to the CPR Project Officer on an as-needed/requested basis. Data is protected during all facets of storage and transmission.

## 5. Technical Components

The CPR system is based on a client/server architecture comprised of three major components. This section identifies the CPR system components and describes how they interact to support the system. *Figure* 1.

*CPR Component Connections (Figure 1)* shows how these components connect and process information.

### 5.1. CPR Workstation (CPR-WS)

The CPR-WS is a single purpose, client workstation, providing authentication and secure communication services for CPR users and cardholders to support PIN reset.

The CPR WS:

- Provides the TASMs and CTAs hands-on access
- Enables user access to the CPR-DS for authentication and to the CPR-PS for the reset process

A CPR-WS is comprised of an IBM-compatible laptop computer using the Windows 2000 operating system, a biometric fingerprint scanner, CAC readers (two each – one for the CPR user; the other for the CAC holder), a numeric keypad, a mouse, and a portable hub.

### 5.2. CPR Portal Service (CPR-PS)

The CPR-PS:

- Is the server infrastructure providing secure CAC lifecycle management, including the PIN reset function

Uses the CPR-DS for authentication prior to allowing user access

The DMDC maintains this server in a secure facility, and provides the necessary PIN reset commands. The CPR-PS uses the CPR-WS for remote access after establishing positive authentication.

### 5.3. CPR DEERS Service (CPR-DS)

The CPR-DS:

- Is the server infrastructure providing DEERS Person Data Repository (PDR) access
- Authenticates users (CTAs and TASMs) via the Sign-on Table (SNT) and authorizes DEERS use

The CPR-DS servers:

- Are located in a secure facility and are accessed remotely via the CPR-WS
- Authenticates TASMs, CTAs, and CAC holders via biometric fingerprint matching and photographic verification of CAC holders.

### 5.4. CPR Management Service (CPR-MS)

The CPR-MS, manages the Navy's day-to-day CPR business processes. It is maintained by the CAC PMO and is completely independent of other CPR system components, although it uses data extracted from the DEERS in an off-line mode.

Under CPR version 1.1, the CAC PMO uses this service to

- Monitor and manage registrations and CPR attempts
- Provide users a locator function to identify the closest CPR capability.

Additional privileges may be granted to TASMs for monitoring transactions with subsequent CPR releases.

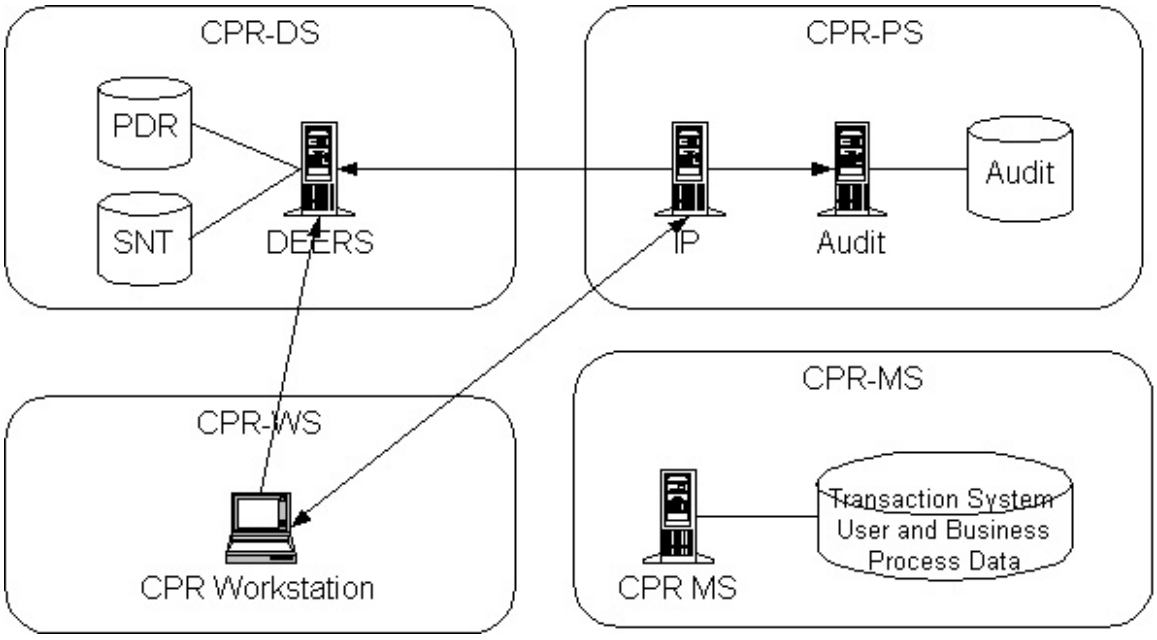


**Figure 1.**

**CPR Component Connections**

# 6. Equipment Fielding

## 6.1. Hardware

### 6.1.1. Initial Fielding

The initial CPR equipment fielding will be via requests from Navy sites to the CPR Project Officer.

### 6.1.2. Spare Component Maintenance

CAC PMO maintains minimal spare components for CPR workstations. Authorized site TASMs shall forward requests for spare components to the CAC PMO.

### 6.1.3. Replacement Fielding

Prior to requesting a workstation replacement, TASMs must ensure that troubleshooting efforts have been completely exhausted through contacting the CAC PMO help desk (see Section 15).

After confirming the need for workstation replacement, the site TASM must coordinate with the CPR project officer to field a replacement.

### 6.1.4. Individual Peripheral Replacement

Workstation peripherals (such as the numeric keypad, card readers, hub, or fingerprint reader) are not forecasted for upgrade on a scheduled basis. However, due to wear and tear, damage, and/or malfunctions, these components may require occasional replacement. Because these components are considered expendable, commands must fund their own replacements unless the items still fall under warranty coverage.

## 6.2. Software

### 6.2.1. Initial Fielding

Software, including the operating system, CPR application, and any other utilities necessary for secure workstation operation are loaded and tested on all CPR workstations prior to shipment.

### 6.2.2. Revisions and Updates

Revisions, updates, and service packs are available for download as they become available. As updates are posted, the CAC PMO will notify TASMs of the availability. The TASMs are then responsible for upgrading all CPR workstations under their control.

# 7. Physical, Procedural, and Personnel Security Controls

## 7.1. Physical Controls

When the CPR workstation is in use, an authorized TASM or CTA must always be present. When not in use, the workstation must have all CACs removed from the card readers.

CPR workstations will be protected against theft, loss, and unauthorized use as described in the next section.

### 7.1.1. Physical Access

TASMs and CTAs will ensure that if the workstation is involved in travel, under no circumstances shall the equipment be left unattended. This includes unattended baggage checking on commercial conveyance (such as an airplane, train, bus or taxi).

The following rules apply to CPR workstation security:

- An approved TASM or CTA must be present any time the CPR workstation is powered up and in use
- TASMs and CTAs must ensure that all CACs are removed from the card readers before securing the workstation.
- Under no circumstances shall TASMs or CTAs share CACs, passwords, or PINs.
- All Navy-accepted property accountability measures will be taken to ensure that TASMs retain custodial oversight and responsibility for the CPR assets under their control. Because many CPR site users may access this equipment, this rule is particularly important. When other CPR site users sign out equipment, it is the TASM's responsibility to ensure the proper documentation (such as a hand receipt) is completed to identify a chain of custody. Further, when CPR equipment is returned to the TASM, it is jointly the responsibility of the TASM/CTA returning the equipment to inspect the asset(s) for damage and proper operation. In the event of damage, appropriate investigation(s) are initiated.

### 7.1.2. Power and Air Conditioning

The following hardware requirements relate to CPR workstation power and temperature control:

- Store the CPR workstation in a dry, preferably temperature-controlled environment
- Use a surge suppressor when the CPR workstation is in use
- Batteries for CPR workstation laptops should be charged prior to use and protected from damage or heat

### 7.1.3. Water Exposures

The CPR workstation shall be located so as to prevent undue exposure to dirt, dust, inadvertent jolting or jarring and water collection/immersion.

#### 7.1.4. Fire Prevention and Protection

Fire extinguishers shall be located in close proximity to CPR assets and associated storage cabinets. The site's disaster recovery plan should include fire disaster recovery procedures.

#### 7.1.5. Media Storage

The CPR workstation requires no anticipated media storage requirements.

#### 7.1.6. Waste Disposal

Normal office waste is periodically removed or destroyed. CPR users will not write down passwords for CPR workstation access. CPR users or CAC holders must not write down their PIN during the reset process, but rather commit the PIN to memory. Any generated paper waste containing sensitive information must be shredded or incinerated immediately following the reset activity.

#### 7.1.7. Emergency Actions

To protect the operational CPR workstation and peripherals from unauthorized use during hostile actions and natural disasters, CPR users must (if they cannot be safely evacuated) physically destroy the CPR equipment or remove and destroy the hard drive.

### 7.2. Procedural Controls

#### 7.2.1. Trusted Roles

Section 2.4 and 2.5 defines the TASM and CTA responsibilities. The procedures for exercising these responsibilities are described throughout this policy statement and in the CAC PIN Reset Standard Operating Procedures and Users' Guide.

#### 7.2.2. Activation Data Protection

Because the PIN that activates CAC applications also provides access to a holder's private PKI keys (and consequently can allow someone to assume the holder's identity), it is imperative that only the CAC holder knows this number. PINs must not be shared among CAC holders or with the TASM or CTA during the reset process.

#### 7.2.3. CPR Workstation Administration

To maintain DMDC security for DEERS/RAPIDS system access, all CPR workstations must meet stringent security requirements as stipulated in the *System Security Authorization Agreement (SSAA)* or the Net Worthiness Certification. Toward that end, CPR workstations assembled by the CPR project Officer are locked down to prevent access to all but the necessary functions required by TASMs to administer other CPR users and perform the PIN reset process.

## 7.3. Personnel Controls

### 7.3.1. Background, Qualifications, Experience, and Clearance Requirements

CPR managers and users must meet the following minimum requirements.

#### Project Officer

The CPR Project Officer must:

- Be a DoD uniformed service member, DoD civilian, or contractor working for the Navy
- Be capable of sending and receiving digitally signed and encrypted email
- Have a working knowledge of the Navy field support structure, including populations and missions of units and sites
- Be familiar with Public Key Infrastructure (PKI), the CAC issuance process, and the Navy's CPR process policy
- Have not been convicted of a felony offense
- Be a United States citizen or hold an active security clearance and have not knowingly been denied a security clearance or have had a security clearance revoked
- Be trustworthy
- Have a minimum of 12 months of retainability

#### TASM

A Trusted Agent Security Manager must:

- Be a U.S. Citizen
- Be a DoD uniformed service member, DoD civilian, or contractor working for the Navy
- Be appointed in writing by an approving authority
- Be capable of sending and receiving digitally signed and encrypted email
- Be a CAC holder
- Have completed requisite CPR TASM training
- Have not been convicted of a felony offense
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Have an active and current National Agency Check (NAC) background investigation
- Be trustworthy
- Be knowledgeable of Navy equipment accountability procedures
- Have a minimum of 6 months of retainability

**CTA**

A CAC Trusted Agent must:

- Be a U.S. Citizen
- Be a DoD uniformed service member, DoD civilian, or contractor working for the Navy
- Be appointed in writing by the (or designated representative) responsible for their site
- Be a CAC holder
- Have completed hands-on CPR training (administered by the site TASM)
- Have not been convicted of a felony offense
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Be trustworthy

### 7.3.2. Background Check Procedures

An organization recommending a TASM appointment must submit a CPR User Qualifications Affidavit (Appendix D) with a request for the TASM Registration/Revocation (Appendix C) signed by the Commanding Officer/Officer in Charge (or designated representative). This affidavit states that the recommended TASM meets the requirements of Section 7.3.1 based on the organization's research, knowledge, and/or interview with the applicant.

# 8. Site Registration

## 8.1. Site Definition

A CPR site is defined as either one or a collection of CPR workstations under the organizational control of the CAC PMO.

Each TASM or CTA is authorized specific rights and privileges within the DEERS/RAPIDS system for assigned site workstations. For this reason, TASMs have administrative privileges only for their site users. They may not administer users from other sites.

## 8.2. TASM Requests to CAC PMO

TASMs are in the best position to determine how to most efficiently deploy CPR capability. Factors such as mission importance, location of large CAC holder populations, headquarters facility priorities, and expected number of PIN resets are factors considered when identifying potential sites.

For situations where TASMs require new or additional CPR capability above initial fielding requirements, see Section 11.

Site registration is initiated by the CPR Project Officer. This is accomplished by completing and forwarding the site ID registration worksheet (see Appendix B**)**. Completing all worksheet fields is required to successfully register a site. The worksheet is completed for each site and subsequently forwarded to CAC PMO CPR Project Officer via a digitally signed email.

## 8.3. CAC PMO Requests to DEERS

After the CPR Project Officer receives the digitally signed email containing site registration data, it is reviewed for proper format and completeness and then forwarded to the DEERS Security Team (DST) for processing.

If site registration requests are not in proper format or are incomplete, the CAC PMO responds to the TASM with the reason and coordinates the corrected request resubmission.

## 8.4. DEERS Turn-Around

The DEERS processes batch changes to site IDs and CPR users on a nightly basis. Allow at least 48 hours for changes to become effective.

## 8.5. Site ID Notification

After successfully establishing site registration, the DST notifies the CPR Project Officer of the new site ID number.

Additionally, after receiving the new site ID information, the CPR Project Officer manually enters the new site ID information into the CPR-MS and notifies the TASM by digitally signed email.

# 9. TASM Registration

## 9.1. TASM Registration Request

TASM registration is initiated by the site Commanding Officer/Officer in Charge (or designated representative). This registration requires completing and forwarding the Request for TASM Registration/Revocation (Appendix C) and the CPR User Qualifications Affidavit (Appendix D) through their service to the CPR Project Officer. Completing all request form fields is required to successfully register the TASM. Each completed TASM request form must be forwarded by the responsible POC to the CPR Project Officer via a digitally signed and encrypted email.

***Note:*** The registration information *must* be sent in via digitally signed and encrypted email format because DEERS registration requires the TASM's Social Security Number.

## 9.2. CAC PMO Request to DEERS

After the CAC PMO receives the digitally signed email containing the TASM registration request form and qualifications affidavit, the CPR Project Officer reviews it for qualification criteria and completeness.

- If the request is suitable, the CPR Project Officer forwards it to the DEERS Security Team (DST) for processing via a digitally signed email.

  ***Note:*** For the first registered site TASM, this information is required to properly configure the site's CPR workstation(s).

- If the request does not meet the qualification requirements or is incomplete, the CPR Project Officer responds with the justification(s) and coordinates resubmitting a corrected request.

## 9.3. DEERS Turn-Around

Allow at least 48 hours for DEERS changes to become effective, since DEERS processes batch changes to site IDs and TASMs on a nightly basis.

## 9.4. TASM Registration Notification

As no DEERS capability currently exists to verify successful registration, CPR user authentication is the sole confirmation method. TASMs must attempt to access the CPR system after a 48-hour period. For new CPR capability at a location, confirmation is not possible until the CPR workstation has been received.

If the individual is the first site TASM, the CPR Project Officer forwards the TASM's information to DMDC (in conjunction with the previously registered site ID) for the site's workstation configuration. Additionally, the CAC PMO contacts the individual through the serving POC via digitally signed email to initiate the site ID survey.

### 9.5. Updating TASM Information

Periodically, TASM demographic information (such as telephone number or email address) requires updating. This is accomplished via TASM update request form submission (see Appendix G) to the CPR Project Officer. Request forms may be submitted by the Commanding Officer/Officer in Charge (or designated representative) or by the TASMs themselves. Forms will be submitted via digitally signed email.

***Note:*** Allow at least 48 hours for DEERS changes to become effective, since the DEERS processes batch changes to site IDs and TASMs on a nightly basis.

### 9.6. Site ID Survey

The primary TASM performs a site ID survey after establishing the site ID and registering for a new site. The TASM obtains local configuration information required to install CPR site workstations.

Appendix F provides a copy of the site ID survey. The TASM submits the completed Site ID survey through the CPR Project Officer via digitally signed email.

### 9.7. TASM Privileges

Registered TASMs have the ability to conduct PIN reset and also administer users on the site's CPR workstation(s).

- *Primary site TASMs,* privileges are enabled through the workstation upon initial configuration.
- *Alternate site TASM* are enabled by the primary site TASM. The primary TASM accomplishes this using the User Administration tool—a component of the CPR software. Additionally, the alternate TASM is provided limited administrative rights using Windows 2000 to create the new TASM's login profile.

### 9.8. Training a New TASM

If the new individual is:

- The first site TASM, training follows procedures specified in Section 2.1 of the CPR Standard Operating Procedures and User's Guide.
- Alternate TASM training follows procedures specified in Section. 2.1 of the CPR Standard Operating Procedures and User's Guide.

### 9.9. Criteria and Procedures for TASM Removal

TASMs are removed from the CPR workstation and privileges revoked from the DEERS under any of the following circumstances.

- Is under investigation (or has been convicted) of any offense punishable by the Uniformed Code of Military Justice (UCMJ) or equivalent civilian law
- Has been relieved of duties
- Has left military service or has otherwise become disassociated with the organization

- Has transferred out

Local Commanders (or their designated representatives) must institute procedures for identifying TASMs requiring removal. Once identified, the POC must be notified as soon as possible.

At least one TASM must be assigned to each site ID to ensure CPR capability. If TASM removal results in capability loss, the local Commander (or designated representative) identifies a replacement TASM for registration.

The local Commander (or designated representative) notifies CPR Project Officer of all TASM revocations via a digitally signed email. CPR Project Officer then coordinates with the DST to ensure timely revocation, using similar procedures as those for TASM registration.

After determining that a TASM should be revoked, the remaining site TASM must immediately remove the individual's local sign-on profile for the operating system from the CPR workstation(s).

The remaining TASM removes the sign-on profile via the CPR's User Administration application. The CPR SOP and User's Guide provides the specific profile removal instructions.

***Note:*** Allow at least 48 hours for DEERS changes to become effective, since the DEERS processes batch changes to site IDs and TASMs on a nightly basis.

.

# 10. Equipment Assembly and Shipment

## 10.1. Building the CPR Workstation

The following prerequisites apply to building and configuring a CPR workstation:

- Establishing a site ID
- Identifying at least one site TASM (the primary TASM)
- Specifying the local configuration (via completing the Site Survey in Appendix F)

Once these actions are completed and all required data is obtained for a site, the CPR Project Officer shall commence the workstation build.

The CPR Project Officer assembles all hardware, installs software, and configures the workstation for the specific site. The CPR Project Officer then tests and evaluates the workstation for quality control standard compliance, and upon successfully passing evaluation, releases the workstation for shipping. Workstations that do not pass testing are returned for rework.

## 10.2. Shipping the CPR Workstation

After successful testing, CPR workstations and associated equipment are packaged for shipment. This includes peripherals, additional software applications, Standard Operating Procedures (SOPs), and CPR user documentation. Additional documentation includes an inspection checklist and setup procedures. An initial password for the primary TASM is generated and sent (via a separate email). This password must be changed upon the TASM's first CPR workstation login.

***Note:*** Although the password allows limited CPR workstation access, it cannot access further functions without an inserted TASM CAC and valid biometric authentication.

## 10.3. Property Accountability

The following describes the property accountability process for a CPR workstation shipment.

1. The CPR workstation shipment is accepted by the office representative authorized by the Commanding Officer/Officer in Charge who in turn notifies the site TASM for equipment pickup.

2. The TASM acknowledges receipt and official custody of the CPR workstation(s) via completion and return (to CPR Project Officer) of the accompanying custodial shipping/transfer receipt.

3. The TASM conducts a physical inspection, performs setup procedures, and tests to verify workstation operation. If all inspections, tests, and configuration procedures are successful, the TASM may begin to administer users and/or conduct PIN resets.

***Note:*** If TASM training is conducted via web-based or hard copy materials, the TASM undergoes this training now. The TASM then completes the TASM and CTA Acknowledgement of Responsibilities Form (Appendix E) and returns it to the CAC PMO as specified in Section 3.

## 11. Request for Additional CPR Capability

For activities requiring CPR capability beyond their initial issuance, contact the CPR project officer for additional or new CPR capability.

### 11.1. Additional CPR Capability

This request applies to sites already having CPR capability; however local authorities (normally the local Commander or TASM) have determined that an insufficient number of workstations exist. The following describes the process for requesting additional CPR capability.

1. The local authority contacts the CPR project officer to initiate an additional capability request. Commanding Officers/Officers in Charge will create their own internal procedures for initiating and reviewing capabilities at the site level.

2. Submit a capability request letter to the CPR project officer, via a memorandum signed by the local Commander (or designated representative) at the existing or potential site. This memorandum must include justification for the additional requirement and specifies whether the equipment is to be funded by the local installation

3. CAC PMO, after completing the review process, takes one of these actions:
    - **Returns the request for additional information**
    - **Disapproves** (returns with rationale)
    - **Approves**

### 11.2. New CPR Capability

New CPR requests apply to sites having no CPR capability and it is not included in approved programmed plans. Local authorities (normally the local Commander) establish requirements/requests for new CPR capability. Commands willing to purchase CPR equipment with their own funds should clearly state this in your request.

Requests for new CPR capability follow the same procedure as that for requesting additional CPR capability (see Section 11.1). However, because no site IDs, site surveys, or registered TASMs are established, these processes must be completed if the CPR Project Officer approves the new capability.

## 12. CTA Registration

Unlike TASMs, CTAs do not have CPR workstation administrative privileges. CTAs:

- Are restricted to PIN reset capability
- Receive training on-the-job (see Section 3). This training may occur at registration time, or since registration may take at least 48 hours, be conducted subsequently.

### 12.1. CTA Identification and Qualifications

Potential CTAs must meet minimum qualifications (see Section 7). Once identified, the TASM must complete and retain a Qualification Affidavit and conduct the CTA registration. An Acknowledgement of Responsibilities form (Appendix E) must also be completed and signed. A copy of this acknowledgement must be forwarded to the CPR Project Officer, with the original copy maintained by the TASM.

### 12.2. TASM CTA Registration

A site TASM registers CTAs directly into the DEERS via the CPR workstation User Administration tool. The CPR Standard Operating Procedures and User's Guide provides specific CTA registration instructions.

***Note:*** Because the DEERS processes batch changes to CPR users on a nightly basis, allow at least 48 hours for changes to become effective. Successful access to CPR confirms the CTA registration.

### 12.3. Updating CTA Information

Periodically, CTA personal information (such as telephone number or email address) may require updating. The site TASM updates this information using the CPR workstation User Administration tool. The CPR Standard Operating Procedures and User's Guide provides specific CTA personal information update instructions.

### 12.4. Criteria and Actions for CTA Removal

A CTA must be removed from the CPR workstation and privileges revoked from the DEERS if the CTA:

- Is under investigation (or has been convicted) of any offense punishable by the Uniformed Code of Military Justice (UCMJ) or equivalent civilian law
- Has been relieved of duty
- Has left military service or has otherwise become disassociated with the organization
- Has transferred out

After determining that a CTA should be removed or revoked, the TASM must immediately remove the individual’s local operating system sign-on profile from the CPR workstation(s).

The local TASM then removes the CTA from the CPR workstation and DEERS access lists via the CPR workstation user administration application. The CPR Standard Operating Procedures and User's Guide provides specific CTA access removal instructions.

Additionally, the TASM then contacts the CPR Project Officer concerning the action. This may be accomplished through digitally signed email, and must include the reason for revocation.

## 13. CAC PIN Reset Process Overview

This CAC PIN reset process overview provides only general information. The CPR Standard Operating Procedures and User's Guid*e* provides specific CPR reset instructions.

### 13.1. Storage and Sign-Out of the CPR-WS

After accepting receipt of the CPR-WS, site TASMs are responsible for site equipment storage, security, and disbursement. Commands must determine the most appropriate means to provide CPR capability to their user community. TASMs will store CPR workstations in a secure location and sign out the equipment to other TASMs and CTAs. Since this is conducted on the local level, TASMs must ensure positive accountability of the equipment. TASMs shall use hand receipts in accordance with standard custodial procedures to ensure this accountability.

### 13.2. Equipment Setup and Power On

The CPR workstation can be deployed as follows to best address the CAC holder user base:

- To a fixed location
- To multiple locations

To perform CPR, the TASM or CTA must connect the workstation using the instructions provided in the CPR Standard Operating Procedures and User's Guide. This includes connecting all peripherals, powering up the workstation, and specifying any local configuration parameters.

### 13.3. TASM/CTA Sign On and Authentication

After connecting and powering on the workstation, the TASM or CTA must sign onto the CPR-WS operating system using their user name and password.

***Note:*** This access information must be protected and never shared with other personnel.

Upon a successful log on, the TASM or CTA must authenticate to the CPR-DS (DEERS System) as follows:

1. The TASM or CTA must insert their CAC into a card reader and enter a PIN to verify identity to DEERS

2. DEERS then conducts a biometric (fingerprint) verification to complete authentication

### 13.4. CAC Holder Authentication

Following successful authentication, the TASM or CTA may perform CAC PIN reset for CAC holders as follows:

1. The CAC holder inserts their CAC into the second reader.

2. The TASM/CTA initiates the reset application, which authenticates the holder via photographic and biometric functions.

3. During each step, the TASM/CTA verifies successful authentication.
    - If successful, the PIN may be reset
    - If not successful, the CTA or TASM can attempt authentication several more times

***Caution:*** If either the photographic or biometric authentication remains unsuccessful, the TASM or CTA instructs the holder to return to the CAC issuance facility for resolution. Attempts of unauthorized access (such as CAC holder impersonation), must be reported immediately. Contact the CAC issuance facility, local information security officer, or CAC Project Officer.

### 13.5. CAC PIN Reset Process

The following process, using the numeric keypad attached to the CPR-WS, describes the CAC PIN reset steps following CAC holder authentication.

1. The TASM or CTA instructs the CAC holder to enter the new PIN using the numeric key pad. This must be a numeric code, 6 – 8 characters long.

2. The CAC holder enters the new PIN.

3. The CPR software generates a verification message upon successful reset. The TASM or CTA should stress the importance of PIN memorization to the CAC holder to prevent recurrence.

***Note:*** TASMs, CTAs, or CAC holders must never share their PIN with other personnel. This includes other TASMs and CTAs during the actual reset process. Every effort should be made to conceal PIN entry.

## 14. CPR Equipment Accreditation

### 14.1. Blanket Accreditation Documentation

Defense Manpower Data Center owns and operates the CPR infrastructure components under the DEERS accreditation; these components are included in the blanket accreditation documentation which governs their use. This accreditation includes all functions within DEERS/RAPIDS and encompasses all communication from the CPR-WS to the CPR-PS and CPR-DS.

## 15. Technical Support Structure

The following technical support structure is established to assist all CPR users in the field.

### 15.1. Help Desk Support

DMDC has Support Centers (help desks) to directly support CAC system users across the spectrum of support requirements. The help desks field calls directly from the CPR Project Officer. TASMs and CTAs who are experiencing any difficulty with the CPR process should contact the CPR Project Officer. This includes workstation configuration, applications, hardware, software and troubleshooting issues related thereto.

Navy Support Center/help desk:

(850) 452-7693 or 452-7809

### 15.2. Web-Based Information

DMDC publishes policies, procedures, known solutions, and tips in the form of Frequently Asked Questions (FAQs), engineering-based solutions, and information from the DMDC knowledge base. When possible, users should consult the DMDC website (www.dmdc.osd.mil) for potential solutions prior to initiating trouble calls. The CAC PMO website (http://pmo.cac.navy.mil) publishes CPR policies, procedures and training.

### 15.3. CPR-MS Information Availability

Although primarily a management tool for the CPR Project Officer during CPR initial fielding efforts, additional capability may be added in subsequent releases to CPR-MS to allow the TASMs to review pertinent CPR information. This informational source will require authentication via CAC PKI certificates and allows these individuals to run CPR statistic queries for their respective areas of control. CAC PMO will notify sites when this capability becomes available.

## Appendix A. Acronyms and Abbreviations

| | |
|---|---|
| CAC | Common Access Card |
| CBT | Computer Based Training |
| COTS | Commercial off the Shelf |
| CPR | CAC Personal Identification Number Reset |
| CPR-DS | CPR DEERS Service |
| CPR-MS | CPR Management Service |
| CPR-PS | CPR Portal Service |
| CPR-WS | CPR Workstation |
| CTA | CPR Trusted Agent |
| DEERS | Defense Enrollment Eligibility Reporting System |
| DMDC | Defense Manpower Data Center |
| DoD | Department of Defense |
| DoN | Department of the Navy |
| FAQs | Frequently Asked Questions |
| ID | Identification |
| PDR | Person Data Repository |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| POC | Point of Contact |
| RAPIDS | Real-time Automated Personnel Identification System |
| SNT | Sign-on Table |
| SOP | Standard Operating Procedures |
| SSAA | System Security Authorization Agreement |
| TASM | Trusted Agent Security Manager |
| VO | Verifying Official |

## Appendix B. Request for Site-ID Registration

### CPR Site Identification Registration Request

From: CAC Program Management Office, CPR Project Officer Date:

To: DEERS Security Team
DEERS/RAPIDS Operations Division
1555 Wilson Boulevard Suite 609
Arlington, Virginia 22209-2593 FAX (703) 578-5198

Subject: **Request for CAC PIN Reset (CPR) Site-ID: Registration ☐ Removal ☐**

**Section I**

Requesting Command:

Point of Contact Last Name: First Name:

Telephone: ( ) - DSN: -

Email address: @

Site Address 1:

Site Address 2:

City: State: Zip Code: Country:

Service/Organization: _____ Navy

Command POC:

Last Name: First Name:

Telephone: ( ) - DSN -

Email address: @

**Section II: (To be completed by CAC PMO)**

Approved by: Date Approved:

**Section III: (To be completed by DEERS Security Office)**

Approved by: Date Approved:

## Appendix C. Request for TASM Registration/Revocation

### CPR Trusted Agent Security Manager
### Registration/Revocation Request

**From:** CAC Program Management Office, CPR Project Officer **Date**:

**To:** DEERS Security Team
DEERS/RAPIDS Operations Division
1555 Wilson Boulevard Suite 609
Arlington, Virginia 22209-2593

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 10 U.S.C. 133 and E.O. 9397

**PRINCIPAL PURPOSE(S):** Collection of social security numbers and other personal identifiers is used to ensure positive identification of individuals in order to successfully register them as CPR users.

**ROUTINE USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use as follows: The "Blanket Routine Uses" set forth at the beginning of OSD's compilation of systems of records notices apply to this system. The Federal and State agencies and private entities, as necessary, on matters relating to securing information during the conduct of official business, utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government facilities, computer systems networks, and controlled areas.

**DISCLOSURE:** Voluntary; however, failure to provide this information will result in failure to register an individual as a CPR user.

**Section I**

**TASM Name:** _____

**Select one:** **Primary TASM**_____ **Alternate TASM**_____

**Social Security Number:** _____ _____

**Telephone:** _____ _____ **DSN:**_____

**Email address:** _____

**Command:** _____

**Address Line 1:**_____

**Address Line 2**_____

**City:** _____ **State:** _____ **Zip Code:** _____

**Action (select one):** **Registration** _____ **Revocation**_____

**Approved/requested by:** _____**Title:**_____

**Telephone:** _____ **DSN:** _____

**Email address:** _____

**Section II: (To be completed by CPR Project Officer)**

**Approved by:** **Date Approved:**

**Section III: (To be completed by the DEERS Security Team)**

**Approved by:** **Date Approved:**

## Appendix D. CPR USER Qualifications Affidavit

**Subject:** CAC PIN Reset (CPR) User Qualifications Affidavit

**To:** CAC Program Management Office, CPR Project Officer

The individual named below been nominated as

( ) Trusted Agent Security Manager (TASM) ( ) CAC Pin Reset Trusted Agent (CTA)

I certify that by use of interviews or other means, I have confirmed that the named individual meets the following qualifications. The nominated individual:

- Is a Common Access Card (CAC) holder
- Is a United States citizen
- Has not been convicted of a felony offense, been knowingly denied a security clearance, or had a security clearance revoked
- Has had a National Agency Check (NAC) background investigation completed
- Is a DoD uniformed service member, DoD civilian, or contractor
- Is capable of sending and receiving digitally signed and encrypted email
- Is trustworthy
- Is knowledgeable of U.S. Navy property accountability procedures
- Has a minimum of six months retainability
- Has a working knowledge of the CPR system and the site to which they are assigned

### CPR User Information

**Name:** _____
(Print)

**Command:** _____

**Email address:** _____ **Telephone:** _____

### Requestor Information

**Name:** _____
(Print)

**Signature:** _____

**Command:** _____ **Title:** _____

**Email address**: _____ **Telephone:** _____

## Appendix E. TASM & CTA Acknowledgement of Responsibilities Form

# TASM & CTA
# Acknowledgement of Responsibilities Form

_____
(Printed name)

has been authorized to receive access to the DEERS system to support your operations as a Trusted Agent Security Manager (TASM) or CAC PIN Reset Trusted Agent (CTA). The information located on your Common Access Card will enable you to gain access to systems for the purpose of CAC PIN Reset. These systems are government property and may only be used for official purposes.

Acknowledgement of Responsibilities: I acknowledge that I have received U.S. Navy approved training to act as a user of the CAC PIN Reset (CPR) system. I understand that as a CPR User, I will be responsible for the following:

- I will conduct TASM or CTA operations in accordance with the stipulations of an approved Navy CPR Business Process Policy Statement and Standard Operating Procedures.
- For TASMs Only: I will ensure that other TASMs and CTAs are trained and capable of continuing CPR capability for the site in my absence.
- I will use my Common Access Card, and the privileges it conveys, only for official purposes.
- I will follow all specified physical security requirements with regards to the protection of the CPR workstation.
- I will not disclose my PIN to anyone or leave it where it might be observed.
- I will never leave the CPR workstation unattended with my CAC inserted into the reader.
- I will report the compromise of my workstation password, or PIN to the appropriate authorities.
- I will report any suspected misuse (attempted or actual) of the CPR workstation to the appropriate authorities.
- I will follow all approved procedures to verify the identity of CAC holders requesting PIN reset.
- For those CAC holders whose identity cannot be verified or authenticated, I will direct them to the nearest DEERS/Rapids CAC Issuance Facility. Additionally, if attempted compromise is suspected, I will contact the CAC Issuance Facility separately to alert them to the situation.
- I will keep a copy of this Acknowledgement of Responsibilities form in compliance with current practices.

Liability: A CPR User will have no claim against the DOD arising from use of the TASM or CTA privileges. In no event will the DOD be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any erroneous PIN reset procedure.

Governing Law: the laws of the United States of America shall govern the CPR process and equipment.

Acceptance: I understand that once I obtain and use my CPR user privileges that I have accepted the authority of the laws and regulations governing those privileges.

**Name:** _____ **Date:** _____
Signature

**Command:** _____ **Site ID #:** _____

**Local Commander or Security Official:** I have personally witnessed the TASM/CTA apply the signature above, and personally verified the identity of the person receiving the CAC PIN Reset User credentials.

**Name:** _____ **Date:** _____
Signature

**Title** _____ **Command:** _____

## Appendix F. Site Survey Worksheet

The information on this worksheet is required to configure CAC PIN Reset workstations for a specific CPR site.

### Site Survey Worksheet

Command: _____

Requested by:_____

Telephone #: commercial_____ DSN_____

Shipping address for the CPR workstation: _____

_____

City: _____ State: _____ Zip Code: _____

---

**If your site uses Static IP assignment as opposed to DHCP, please fill out remainder of Worksheet.**

IP Address Range for CPR workstations (as assigned by the local system administrator)

- - - Through - - -

Internet gateway IP address (as determined by the local system administrator)

- - -

Additional security requirements for access to the Internet from your site (consult your local system administrator and explain):

## Appendix G. TASM Information Change Request

# CPR Trusted Agent Security Manager
# Change Request

From: CAC, PMO, CPR Project Officer Date:_____

To: DEERS Security Team
DEERS/RAPIDS Operations Division
1555 Wilson Boulevard Suite 609
Arlington, Virginia 22209-2593

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 10 U.S.C. 133 and E.O. 9397
**PRINCIPAL PURPOSE(S):** Collection of social security numbers and other personal identifiers is used to ensure positive identification of individuals in order to successfully register them as CPR users.
**ROUTINE USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use as follows: The "Blanket Routine Uses" set forth at the beginning of OSD's compilation of systems of records notices apply to this system. The Federal and State agencies, private entities, as necessary, on matters relating to securing information during the conduct of official business, utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government facilities, computer systems networks and controlled areas.

**DISCLOSURE:** Voluntary; however, failure to provide this information will result in failure to register an individual as a CPR user.

**Section I**

Site ID: _____

Command: _____

TASM Name:_____

Social Security Number:_____ Designation: Primary ☐ Alternate ☐

Telephone: (___) _____ - _____ DSN: _____

Email address: _____

Site Address:

_____

_____

City:_____ State: _____ Zip Code: _____ Country: _____

Section II: (To be completed CAC PMO)

Approved by: _____ Date Approved: _____

Section III: (To be completed by the DEERS Security Team)

Approved by: _____ Date Approved: _____

**Appendix H.** Points of Contact

*CNI, CAC Program Management Office*
SPAWARSYSCEN Charleston, Pensacola Office
Pensacola, FL 32508
(850) 452-7809

**Navy CPR Help Desk: (850) 452-7715/452-7809**